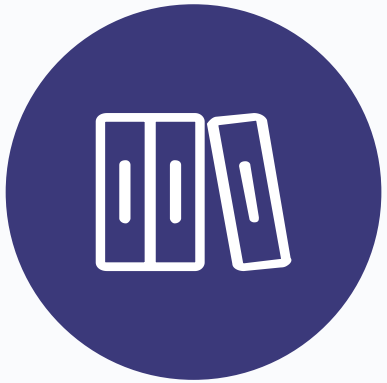


第9章 数据安全销毁

成都信息工程大学 白杨 副教授

2024年X月X日

第9章 数据安全销毁

本讲内容概要：

01 第一节—数据销毁介绍

02 第二节—数据销毁分类

03 第三节—网络数据销毁

第9章 数据安全销毁

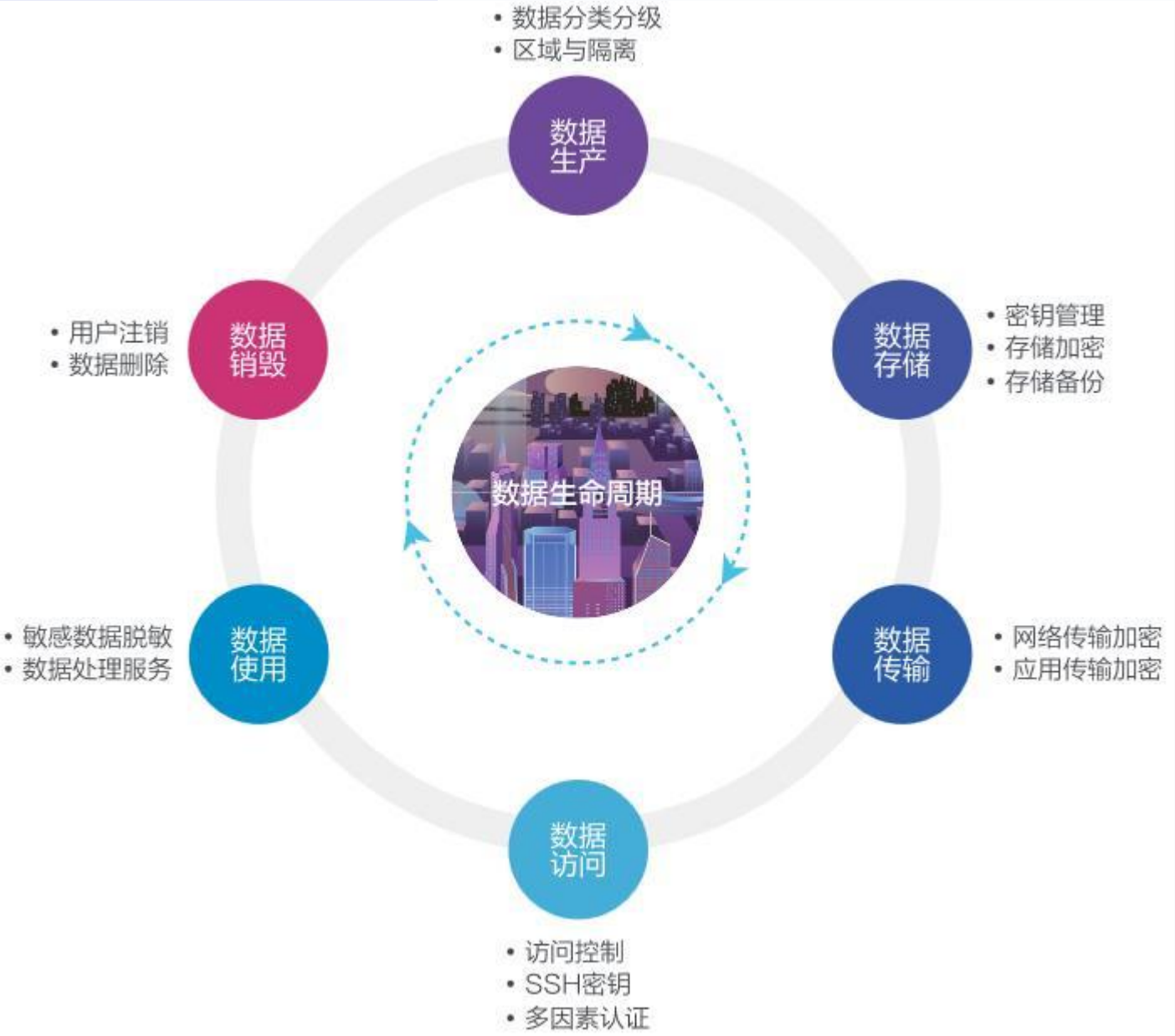
本讲内容概要：

01 9.1.1 数据销毁概述

数据安全生命周期的管理过程包括对数据进行识别与分类、采集、存储、处理、传输、共享与交换、使用、存档以及销毁等连续的阶段，旨在确保数据在整个存在周期内的安全性、完整性和合规性。在数据安全生命周期的管理过程中，数据销毁环节是确保信息长期保密性和完整性的关键步骤。

数据销毁是指采用各种技术手段将存储设备中的数据予以破坏或彻底删除，以确保数据无法被恢复，避免信息泄露，从而维护数据安全和隐私保护的过程。

01 9.1.1 数据销毁概述



01 9.1.2 数据销毁标准

2022年工信部网安第166号文件的第二十条指出，工业和信息化领域数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。

一些国际标准

NIST 800-88

美国国家标准与技术研究院发布的指南，旨在帮助组织和系统所有者根据信息的保密性分类做出合理的媒体清洗决策。

BSI TR-03125

德国信息技术安全局（BSI）发布的数据销毁指南。

ISO/IEC 27001

国际标准化组织(ISO)标准明确指出，存储在信息系统、设备或任何其他存储介质中的信息，当不再需要时，应予以删除。

01 9.1.2 数据销毁标准

A.美国国家标准与技术研究院(NIST)指南

NIST 800-88是美国国家标准与技术研究院发布的指南，旨在帮助组织和系统所有者根据信息的保密性分类做出合理的媒体清洗决策。**该指南提供了从确定媒体类型到选择适当的清洗方法（包括清除、清洗和销毁）的全面流程，并强调了验证清洗效果的重要性，**同时考虑了新兴存储技术对传统清洗方法的影响，确保敏感数据在媒体处置或重用前得到有效保护。

01 9.1.2 数据销毁标准

B.德国信息技术安全局(BSI)标准

BSI TR-03125是德国信息技术安全局（Bundesamt für Sicherheit in der Informationstechnik，简称BSI）发布的数据销毁指南。这份指南为组织提供了关于如何安全销毁存储介质上的数据的指导，以确保敏感信息不会在数据销毁后被恢复和滥用。

BSI TR-03125指南涵**盖了多种数据销毁方法，包括物理销毁和逻辑销毁两种主要类型。物理销毁方法通常涉及将存储介质物理破坏到无法恢复的程度，例如通过消磁、粉碎、熔炼或机械压碎等方式。逻辑销毁则通常指通过数据覆写、重刻录或其他技术手段，使得存储在介质上的数据变得不可恢复。**

该指南还强调了在数据销毁过程中遵守法律法规的重要性，包括数据保护法规和相关的安全标准。此外，BSI TR-03125还可能提供了关于如何评估不同数据销毁方法的适用性、如何选择合适的销毁工具和流程、以及如何记录和审计数据销毁活动的指导。

01 9.1.2 数据销毁标准

C.国际标准化组织(ISO)标准

1．ISO/IEC 27001 信息安全管理

ISO/IEC 27001是一个国际标准，专门针对信息安全管理体系（Information Security Management System，简称ISMS）的建立、实施、维护和持续改进。该标准由国际标准化组织（ISO）和国际电工委员会（IEC）共同制定，旨在帮助组织通过采用一套系统的方法来管理和保护信息资产，确保数据的安全性、完整性和可用性。

该标准明确指出，存储在信息系统、设备或任何其他存储介质中的信息，当不再需要时，应予以删除。这要求组织制定和实施适当的数据销毁政策和程序，以确保敏感数据在不再需要时能够被安全地销毁，防止未经授权的访问和数据泄露。

01 9.1.2 数据销毁标准

2．ISO/IEC 29100 隐私框架

ISO/IEC 29100是一个由国际标准化组织（ISO）和国际电工委员会（IEC）共同发布的隐私框架标准，旨在为组织提供一个全面的隐私保护框架。该标准的核心目的是帮助组织在信息和通信技术（ICT）环境中处理个人身份信息（PII）时，确保隐私权得到适当的管理和保护。

ISO/IEC 29100标准强调了在数据不再需要时，应采取适当的措施来确保数据的安全销毁。这包括但不限于：

1)数据最小化：只收集、使用和保留实现特定目的所必需的数据。

2)数据保留限制：根据法律、法规和业务需求，设定数据的保留期限，并在数据不再需要时进行销毁。

3)数据销毁方法：采用适当的数据销毁技术，如物理销毁（例如粉碎、熔炼）或逻辑销毁（例如数据覆写、加密擦除），以确保数据不可恢复。

4)销毁过程的记录和验证：记录数据销毁的过程，并在必要时进行验证，以证明数据已被安全销毁。

01 9.1.2 数据销毁标准

3.行业标准

金融数据销毁的特殊要求

金融数据销毁的特殊规定着重于在数据不再需要或需依法销毁的情况下，金融机构应采取的措施。**这些规定要求确保数据被彻底删除，以防止数据恢复或未授权访问。对于存储介质上的数据，可能需要采取物理销毁（如粉碎或熔炼）或逻辑销毁（如数据覆写或加密擦除）的方法。同时，要求金融机构记录销毁过程并对销毁效果进行验证，确保数据安全销毁。**

医疗信息的敏感性与销毁流程

医疗信息的敏感性在于其包含个人健康数据、病历信息等高度敏感的个人信息。根据《个人信息保护法》，医疗健康信息被视为敏感信息，需要特别保护。**在数据销毁流程中，医疗机构必须采取确保数据无法还原的销毁方式，以防止数据泄露或未经授权的访问。销毁方法可能包括物理销毁（如粉碎、熔炼）和逻辑销毁（如数据覆写、加密擦除）。此外，医疗机构还需记录销毁过程，并对销毁效果进行验证，确保数据安全销毁。**

01 9.1.2 数据销毁标准

3.行业标准

电子健康记录(EHR)的数据销毁

电子健康记录（EHR）的**数据销毁标准要求医疗机构在EHR不再需要或依法应当销毁时，采取适当的销毁措施。EHR中的数据通常包括患者的个人身份信息、病史、治疗记录等，因此对数据销毁的要求尤为严格。**医疗机构应根据相关法律法规和行业标准，制定详细的数据销毁政策和程序，包括数据的识别、分类、销毁方法选择、执行和验证等步骤。销毁方法同样可能涉及物理销毁和逻辑销毁，且必须确保销毁后的数据不可恢复，以充分保护患者的隐私权益。

01 9.1.2 数据销毁标准

3.行业标准

云服务提供商的数据销毁责任

云服务提供商在数据销毁方面承担着重要的责任。根据客户的要求，**云服务提供商需要确保存储在云平台上的数据能够在合同结束或数据不再需要时被彻底销毁。这包括所有位置和形式的数据，如虚拟机、数据库、备份等。云服务提供商应提供透明的数据销毁流程，并允许客户或第三方进行审计，以验证数据销毁的效果。**例如，华为云在其数据安全白皮书中提出了数据安全责任共担模型，明确了云服务提供商和客户在数据保护方面的责任边界，强调了双方在数据销毁过程中的共同责任。

各国权威机构提出的**数据销毁标准旨在引导组织和个人在处理敏感信息时采取适当的数据销毁措施，以确保信息安全和隐私保护**。在不同的应用场景中，选择符合标准的数据销毁方法能够有效降低信息泄露的风险，维护数据安全和隐私。这些标准通常包括数据销毁的具体步骤、技术要求和操作规范，以确保数据在销毁过程中彻底消除，不留任何可恢复的痕迹。遵循权威机构提出的数据销毁标准，有助于建立起全面的数据安全保障体系，有效应对日益严峻的信息安全挑战，保护个人隐私和敏感信息不受侵犯。

01 9.1.3 数据安全销毁的重要性

在当前数字化时代，大量个人和机构数据包含着大量敏感信息和隐私数据，若这些数据在不再需要时未经妥善销毁，将面临被恶意获取、泄露或滥用的风险。对于国家来说，数据安全销毁有助于维护国家机密和重要信息的安全，防止敌对势力获取敏感数据从而损害国家利益。对于组织来说，数据安全销毁能够保护企业的商业机密和客户信息，避免遭受数据泄露带来的声誉损失和法律责任。数据泄露可能导致个人隐私泄露、金融欺诈等问题，对企业的声誉和经济利益造成严重影响。

因此，数据销毁不仅是技术操作，更是一项重要的信息安全措施。通过数据销毁，可以有效防止敏感信息被不法分子获取，保护个人隐私和企业机密不受侵犯。

第9章 数据安全销毁

本讲内容概要：

01 第一节—数据销毁介绍

02 第二节—数据销毁分类

03 第三节—网络数据销毁

02 9.2 数据销毁分类

物理销毁

物理销毁，又称硬销毁，是一种通过外力或其他物理手段对数据存储介质进行损坏的方式，以确保数据被永久删除并无法恢复。这种方法可以包括破坏硬盘、碾压光盘等手段，以彻底销毁数据，防止数据泄露和不当使用。

逻辑销毁

逻辑销毁是指通过软件或硬件工具对数据进行处理，以覆盖或删除数据，使其无法被读取或恢复。

逻辑销毁根据存储介质分为对磁盘、内存、光盘的数据销毁。

02 9.2.1 物理销毁法

消磁法

消磁法是通过强磁场作用，使存储介质上的磁性记录被完全破坏，从而达到数据销毁的目的。

优点：

> 快速高效，适用于大批量数据销毁。
> 可以处理硬盘、磁带等磁性存储介质。

缺点：

> 仅适用于磁性介质，对非磁性介质无效。
> 设备成本较高。

应用场景：银行、金融机构等需要销毁大量敏感数据的场合。

02 9.2.1 物理销毁法

捣碎法

捣碎法是通过机械手段将存储介质粉碎，使其无法再被使用和恢复数据。

优点：

> 物理破坏彻底，数据无法恢复。
> 适用于各种存储介质，包括硬盘、光盘、固态硬盘等。

缺点：

> 设备操作可能产生噪音和碎片，需要额外的安全防护措施。
> 无法处理已经备份或复制到其他介质上的数据。

应用场景：政府机构、军事部门等需要确保数据绝对安全销毁的场合。

02 9.2.1 物理销毁法

焚毁法

焚毁法是通过高温焚烧的方式将存储介质及其上的数据彻底销毁。

优点：

> 数据彻底销毁，无法恢复。
> 可以处理纸质文件、光盘等不易通过其他方法销毁的介质。

缺点：

> 焚烧过程可能产生有害气体和污染物，需要环保处理措施。
> 操作环境和设备要求较高，需专业设施。

应用场景：医疗机构、研究机构等需要销毁涉及隐私或机密数据的场合。

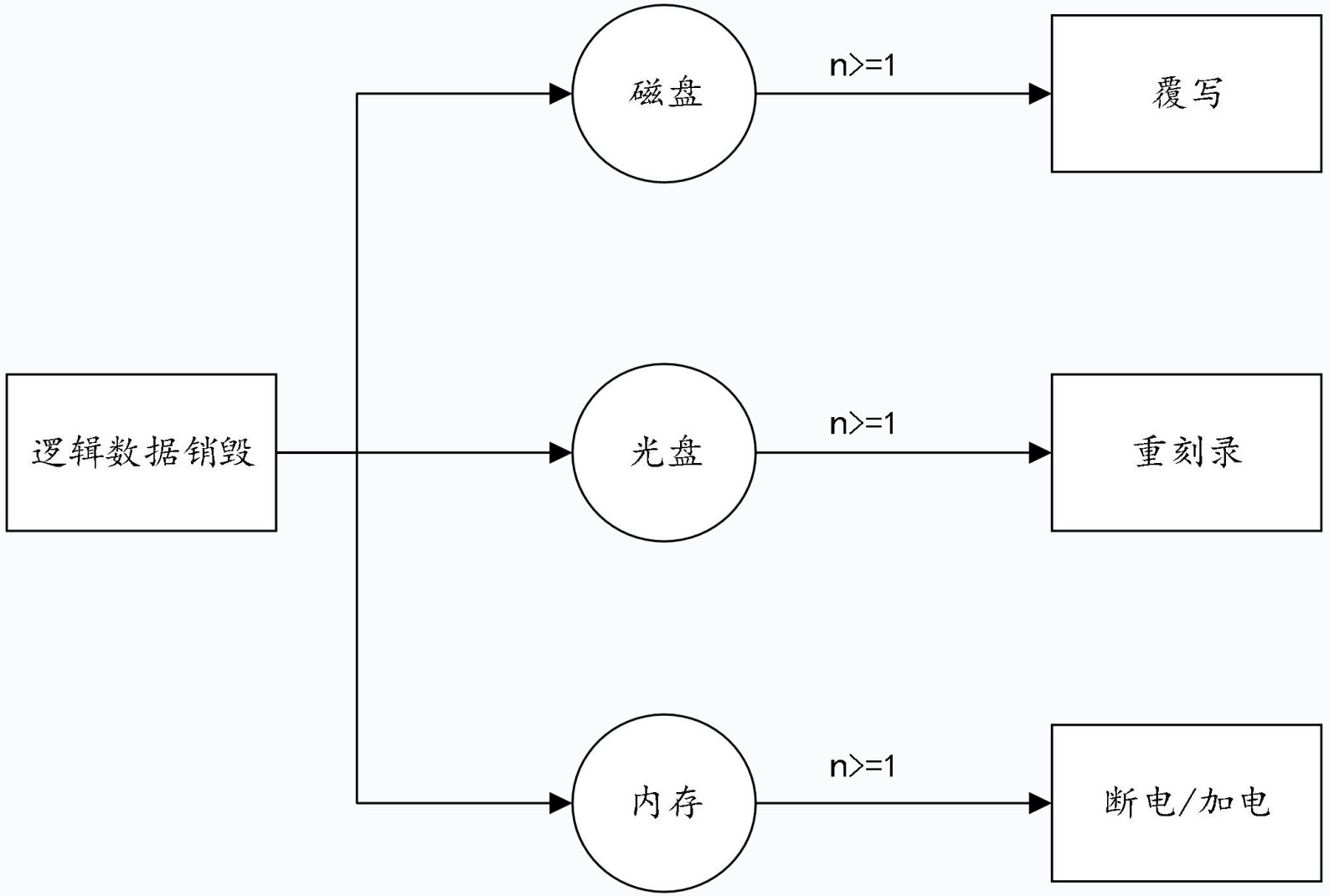
02 9.2.2 逻辑销毁法

逻辑销毁原理

删除和格式化操作是计算机用户最常用的两种清除数据的方式，但其实他们并不是真正意义上的数据销毁方法。

以Windows系统为例，无论磁盘的文件系统采用的是FAT还是NTFS格式，其文件存储时都是将文件分为两个部分：文件目录索引和文件数据实体。删除文件就是系统在目录索引部分将文件标记为已删除，并将该文件所占用的簇标记为可用，从而让文件系统“误以为”该文件已经被清除了，事实上被删除的文件数据实体依然完好地存放在磁盘上。在Linux文件系统中，使用索引节点(inode)来记录文件信息，文件的实际内容存储在磁盘的数据块中，Linux文件系统通过索引节点中的指针来定位这些数据块的位置。当文件被删除时，通常的做法是将该文件的索引节点标记为不再使用，而数据块中的内容并不会立即被清除。

02 9.2.2 逻辑销毁法



02 9.2.2 逻辑销毁法

覆写法

磁盘作为一种外部存储设备，数据以磁场的形式存储在磁性材料上。当数据被写入磁盘时，磁性材料的磁性被改变，从而记录了数据的信息。

销毁磁盘数据的思想就是向需要销毁的数据所在的磁盘扇区中反复写入无意义的随机数据，比如“0”，“1”比特，覆盖并替换原有数据，达到数据不可读的目的。由于磁盘上的数据是以磁场形式存储的，一旦数据被覆盖，原数据的磁场信息会被新数据覆盖，使得原数据几乎无法被恢复。

02 9.2.2 逻辑销毁法

重刻录

重刻录是一种数据销毁方法，通过再次使用激光技术将光盘表面重新刻录，覆盖原有数据，使原数据无法被恢复。重刻录可以有效销毁光盘上的数据。重刻录过程中，新的数据会覆盖原有数据的凹坑和平整区域，使原数据信息被破坏，难以恢复。多次重刻录可以确保数据被有效销毁。

02 9.2.2 逻辑销毁法

断电/加电

内存是计算机中的一种易失性存储器，即在断电后数据会丢失。这意味着内存中存储的数据需要持续电源供应才能保持，一旦断电，数据将会被清除。**通过断电来销毁内存中的数据**是一种简单且常见的方法。当计算机断电后，内存中的数据会迅速消失，无法被恢复。这种方法适用于临时数据或需要临时销毁的数据场景。另一种方法是通过加电来销毁内存中的数据。在某些情况下，可以通过给内存加电来强制清除其中的数据，使其无法被访问。这种方法通常需要专业设备和操作，用于处理对数据安全要求较高的情况。

第9章 数据安全销毁

本讲内容概要：

01 第一节—数据销毁介绍

02 第二节—数据销毁分类

03 第三节—网络数据销毁

03 9.3 网络数据销毁

基于密钥销毁数据

基于密钥销毁的数据不可用销毁方式是一种不销毁数据本身而是销毁加密数据密钥的方式实现数据的不可访问，将数据销毁问题转移至密钥销毁问题。

基于时间过期机制销毁数据

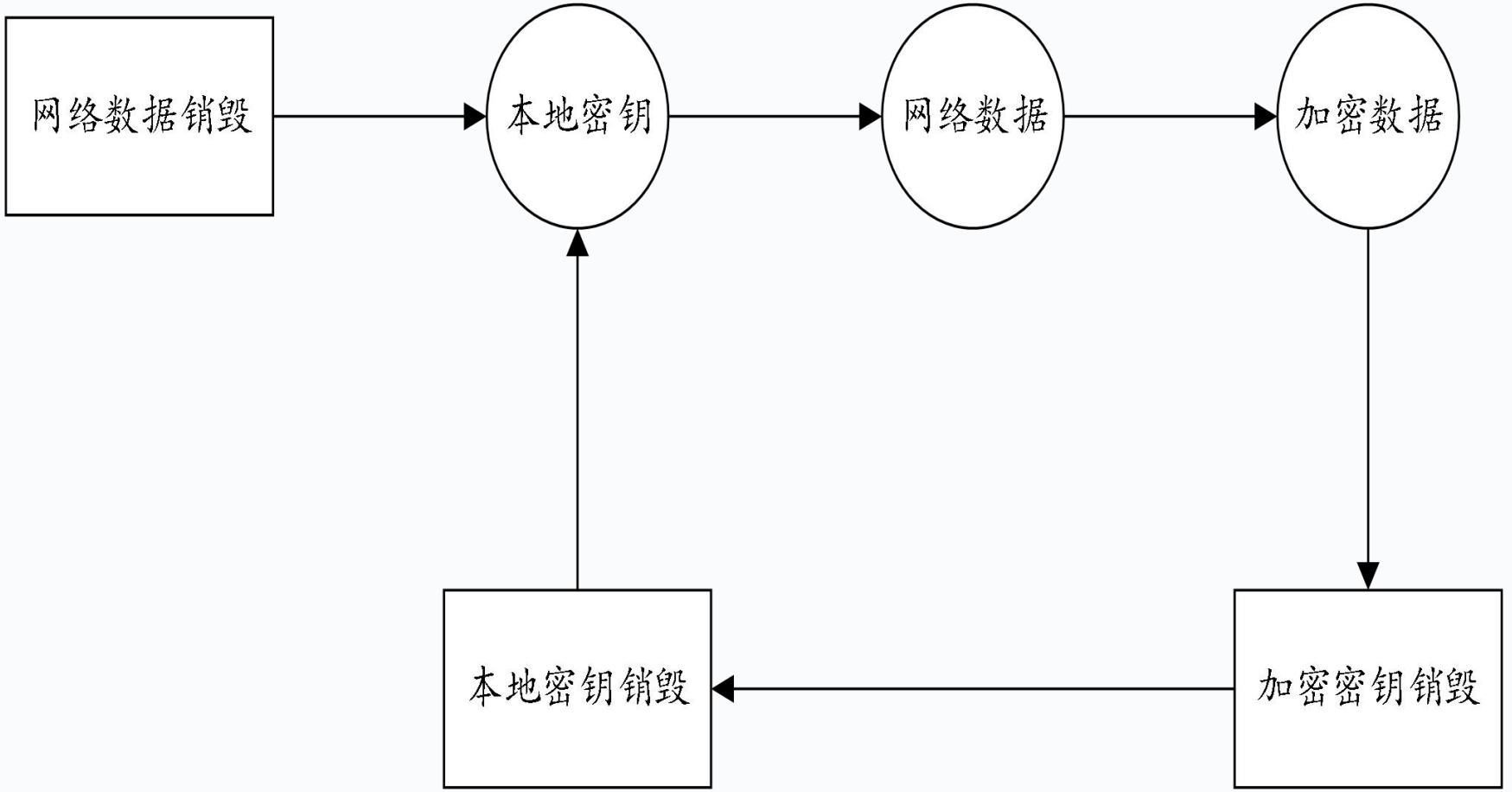
在网络存储中或者与其连接的其他环境中安装一个数据自销毁程序，在数据销毁前对数据打上一个过期时间标记，然后对网络数据进行删除销毁。

72%

网络数据销毁，目前存在两种主要有效的数据销毁方式

03 9.3.1 基于密钥销毁数据

组织机构可以将密钥存储在本地，当需要进行数据销毁操作时，首先对被销毁的数据使用密钥进行加密，然后进行数据销毁操作，最后再将本地存储的密钥进行销毁。



03 9.3.1 基于密钥销毁数据

1、数据加密

首先，对需要销毁的数据进行加密处理，使用密钥将数据转换为密文，确保数据在存储或传输过程中不被未授权访问。

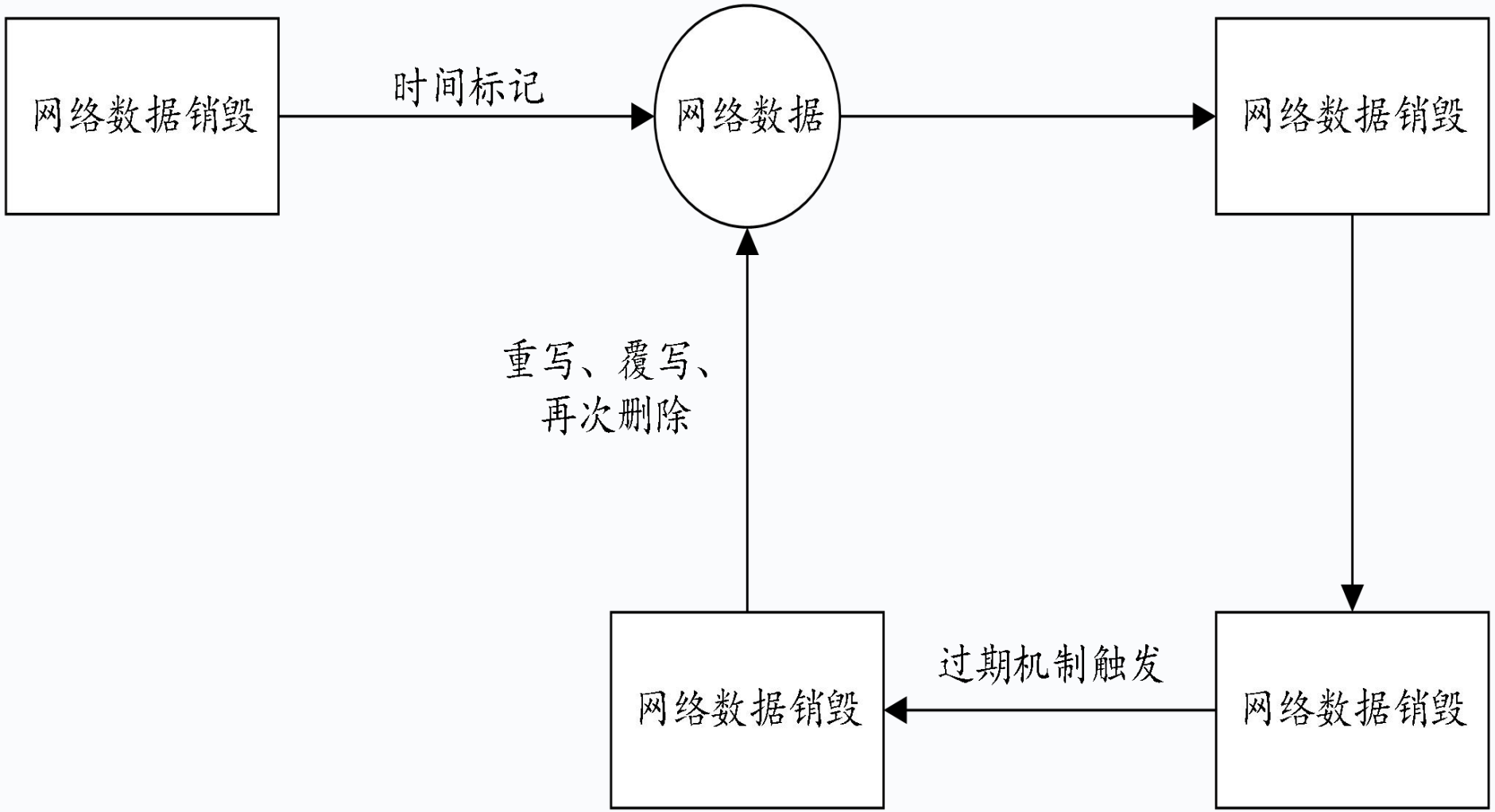
2、密钥管理

密钥管理是关键步骤，需要确保密钥的安全性，只有授权的人员可以访问密钥。在需要销毁数据时，密钥会被销毁。

3、数据销毁

一旦密钥被销毁，原始数据就无法再被还原，实现了数据的永久性删除。

03 9.3.2 基于时间过期机制销毁数据



03 9.3.2 基于时间过期机制销毁数据

在网络存储中，或者与其连接的其他环境中，安装一个数据自销毁程序，在数据销毁前对数据打上一个过期时间标记，然后对网络数据进行删除销毁操作。当攻击者通过数据恢复或其他途径访问已销毁的数据时，一旦数据自销毁程序根据时间标记信息监测到其为过期数据的访问，就会立即启动数据重写、覆写、再次删除等销毁操作，这时，攻击者便无法正常访问已被销毁的数据，从而确保了网络数据销毁的安全性。

谢谢！